UNIVERSIDADE EVANGÉLICA DE GOIÁS
CURSO DE DIREITO
ANDREIA LIMA DE OLIVEIRA

Pedofilia no âmbito virtual

RUBIATABA/GO
2024

ANDREIA LIMA DE OLIVEIRA

Pedofilia no âmbito virtual

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Universidade Evangélica de Goiás- Campus Rubiataba, sob orientação do Prof. Me. Rogério Gonçalves Lima.

RUBIATABA/GO
2024

ANDREIA LIMA DE OLIVEIRA

Pedofilia no âmbito virtual

Monografia apresentada como requisito parcial à conclusão do curso de Direito da Universidade Evangélica de Goiás- Campus Rubiataba, sob orientação do Prof. Me. Rogério Gonçalves Lima.

MONOGRAFIA APROVADA PELA BANCA EXAMINADORA EM 16 / 02 /2024

Mestre Rogério Gonçalves Lima
Orientador
Professor da Faculdade Evangélica de Rubiataba

Mestre Edilson Rodrigues
1 Examinador
Professor da Universidade Evangélica de Goiás- Campus Rubiataba

Mestre Francinaldo Soares de Paula
2 Examinador
Professor da Universidade Evangélica de Goiás- Campus Rubiataba

Dedico essa monografia primeiramente a Deus, por ter me dado sabedoria para a conclusão deste trabalho, a meu pai Valdeci Antônio (in memoriam), a minha mãe Nilvia Maria e as minhas irmãs Verônica e Vanessa que sempre me apoiaram e acreditaram em meu potencial.

AGRADECIMENTOS

Gostaria de expressar minha sincera gratidão a todas as pessoas que contribuíram para a realização deste trabalho. Primeiramente, a Deus que é o autor da minha vida e o responsável pela sabedoria dada para realização desta pesquisa.

À minha mãe, Nilvia, que sempre acreditou em mim e na realização deste sonho.

Às minhas irmãs Verônica e Vanessa pelo apoio incondicional, compreensão e incentivo ao longo de toda a jornada acadêmica.

Minha gratidão ao meu orientador Prof. Me. Rogério Gonçalves Lima e ao Professor e Coordenador Claudio Kobayashi pela orientação dedicada, paciência e valiosas sugestões que foram essenciais para o desenvolvimento deste trabalho.

Por fim, agradeço a todas as fontes de inspiração que tornaram possível a realização deste trabalho. Que cada contribuição, por menor que seja, seja reconhecida e valorizada.

EPÍGRAFE

"Teu dever é lutar pelo direito; porém, quando encontrares o direito em conflito com a justiça, luta pela justiça."

Eduardo Couture

RESUMO

Os objetivos desta monografia é analisar se há limitações no combate aos crimes de ciberpedofilia (pedofilia no ambiente virtual), investigar como o Estado age para identificar os agentes criminosos virtuais e aplicar a devida punição prevista no Ordenamento Jurídico Brasileiro. Para o atingimento desses objetivos, desenvolveu-se o estudo do método dedutivo. Partindo de pressupostos iniciais, busca-se chegar a uma conclusão explorando a interação do tema com a luta contra a pedofilia, especialmente no âmbito virtual. Além disso, buscou-se analisar jurisprudências acerca do tema, legislação vigente, artigos e doutrinas relacionadas ao assunto. Ressalta-se que o crime de pedofilia já era comum, porém, após os avanços tecnológicos, esse crime passou acontecer também de forma virtual e, devido o anonimato e a possibilidade de armazenar dados pornográficos em servidores na *internet*, diminui as chances de encontrar os criminosos e a aplicação de punição. Assim, focando na problemática de identificar se as ferramentas de investigação existentes tem sido eficaz para identificar os agentes criminosos dos crimes de pedofilia no âmbito virtual, foi possível responder sobre a ineficácia perante a identificação de pedófilos virtuais.

Palavras-chave: Direito; Estado; Pedofilia.

ABSTRACT

The objectives of this monograph are to analyze whether there are limitations in combating cyberpedophilia crimes (pedophilia in the virtual environment), investigate how the State acts to identify virtual criminal agents and apply the appropriate punishment provided for in the Brazilian Legal System. To achieve these objectives, the study of the deductive method was developed. Starting from initial assumptions, we seek to reach a conclusion by exploring the interaction of the topic with the fight against pedophilia, especially in the virtual sphere. Furthermore, we sought to analyze jurisprudence on the topic, current legislation, articles and doctrines related to the subject. It should be noted that the crime of pedophilia was already common, however, after technological advances, this crime also began to occur virtually and, due to anonymity and the possibility of storing pornographic data on servers on the internet, the chances of finding the perpetrators decrease. criminals and the application of punishment. Thus, focusing on the problem of identifying whether the State has sufficient technological apparatus and tools to identify the criminal agents of pedophilia crimes in the virtual sphere, it was possible to respond to the ineffectiveness in identifying virtual pedophiles.

Keywords: Law; State; Pedophilia.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ART	Artigo
CF	Constituição Federal
CID	Classificação Internacional de Doenças
CPB	Código Penal Brasileiro
CPF	Cadastro de Pessoas Físicas
ECA	Estatuto da Criança e do Adolescente
IP	Endereço de Protocolo de Internet
LGPD	Lei Geral de Proteção de Dados
Nº	Número
OMS	Organização Mundial da Saúde
RG	Registro Geral
STJ	Supremo Tribunal de Justiça

LISTA DE SÍMBOLOS

§	Parágrafo
#	Hashtag

SUMÁRIO

1. INTRODUÇÃO

Percebe-se que a revolução cibernética-tecnológica, especificamente, o advento da rede digital e do ciberespaço[1] tem propiciado uma comunicação densa e rápida em nível global. Em outras palavras, toda essa revolução tecnológica possibilitou que pessoas de diferentes localidades, idades, etnias e culturas comunicassem umas com as outras, compartilhando suas percepções e experiências de vida. Assim, vertiginosamente, o espaço virtual vem rompendo as fronteiras do espaço real. Todo esse cenário contribuiu para mudanças nos vínculos de amizade, relacionamentos amorosos, estudos, trabalhos e até mesmo no mundo criminal.

Nessa perspetiva, com o avanço da rede, houve também o surgimento de crimes virtuais, entre eles, a pedofilia. Diante disso, é imprescindível compreender a pedofilia tanto no olhar do ordenamento jurídico brasileiro, seu enquadramento nos crimes sexuais contra crianças e adolescentes, quanto na análise do perfil do sujeito que pratica a pedofilia. Assim, é de extrema importância a adaptação do Direito em relação aos crimes virtuais, para que haja controle dos crimes advindos do ambiente virtual.

Conceitua-se crimes cibernéticos aqueles cometidos na *internet*. Esses crimes podem atingir várias pessoas ao mesmo tempo, em diversos lugares e, consequentemente, isso dificulta a identificação do agente que está por trás das redes.

Nesse sentido, denomina-se pedofilia virtual os crimes que ocorrem na *internet*. Esses consistem em produzir, disseminar, adquirir ou armazenar pornografia infantil pelos meios virtuais. Isso ocorre por meio de páginas da *Web* e redes sociais, dentre elas se destacam: *Facebook, YouTube, WhatsApp, Instagram, WeChat* e salas de bate-papo(*chat*).

A pedofilia é um crime grave que se disseminou com muita rapidez e traz indignação da população e, além disso, tem várias consequências. Por intermédio da pedofilia virtual também entra em questão o estupro virtual e pornografia infantil. O Estatuto da Criança e do Adolescente trata de delitos relacionados com a pornografia infantil. A lei nº 11.829/08 alterou a Lei nº 8.069/90 a fim de aprimorar o combate à produção, venda e distribuição de pornografia

[1] Para compreender melhor acerca desse assunto, consulte o seguinte *sítio*: https://www.infoescola.com/internet/ciberespaco/

infantil, assim como criminalizar a aquisição e a posse de tal material e várias outras condutas relacionadas à pedofilia na *internet*. Note que, ainda, o uso da *internet* é um ambiente propício para incitação à prática de atos infracionais contra crianças ou adolescentes para a sua exposição de maneira pornográfica.

Assim, o presente estudo busca responder a seguinte problemática: As ferramentas de investigação existentes tem sido eficaz para identificar os agentes criminosos dos crimes de pedofilia no âmbito virtual?

Os objetivos gerais do trabalho são: analisar se é possível identificar quem são os agentes criminosos que agem por trás dos ataques cibernéticos.

E, como objetivos específicos: analisar as limitações das autoridades diante os crimes no ambiente virtual.

No que diz respeito ao conteúdo, a pesquisa analisará os fatores relacionados ao ordenamento jurídico brasileiro e a atuação do Estado diante o crime de pedofilia virtual. Para chegar as respostas pretendidas, será utilizado o método de pesquisa dedutivo, de onde parte das premissas iniciais para concluir o tema. Assim, será realizada uma comparação da eficiência do Estado e do ordenamento jurídico brasileiro, entendendo como o crime de pedofilia virtual são abordados e solucionados a fim de verificar se as legislações existentes permeiam uma eficácia ou não.

A pesquisa foi realizada em um estudo com base em pesquisas em livros e trabalhos acadêmicos e científicos, bem como a jurisprudência.

O primeiro capítulo do trabalho terá o objetivo de discorrer e analisar os conceitos gerais da pedofilia e seus reflexos jurídicos, na qual, a pedofilia é uma conduta sexual, onde o agente realiza práticas sexuais perante crianças e adolescentes e analisar quais as leis e tipificações penais a fim de punir esse crime.

O segundo capítulo analisará o combate aos crimes de pedofilia virtual e quais são os meios legais para o enfrentamento e métodos utilizados para combate desse crime recorrente no âmbito virtual. Ademais, também será debatidocomo a justiça enfrenta esses crimes para que haja uma punição adequada ao criminoso e se essas condutas são repreendidas pela justiça, com intuito de coibir ações de pedofilia.

O terceiro e último capítulo tratará da responsabilidade das autoridades legais do

Estado e as limitações tecnológicas para a identificação dos criminosos virtuais e a ineficiência de proteção por parte do Estado. Além disso, também serão debatidos as formas céleres para a identificação dos agentes que cometem essa prática delituosa, ou seja, os meios de utilização, quais ferramentas e mecanismos tecnológicos. Assim, cabe ao Estado a proteção, a integridade e a dignidade sexual de crianças e adolescentes.

2. PEDOFILIA E A LEGISLAÇÃO BRASILEIRA

A pedofilia não tem uma "origem" única. Ademais, é importante esclarecer alguns pontos: A pedofilia é uma orientação sexual em que um adulto sente atração sexual por crianças pré-púberes, geralmente, menores de 13 anos. Não é uma orientação sexual aceitável e nem legal, pois envolve comportamento sexual com crianças, o que é ilegal em praticamente todas as jurisdições do mundo devido ao dano que causa às crianças.

É crucial definirmos o conceito de pedofilia. Desde a década de 1960, a Organização Mundial da Saúde (OMS) trouxe na Classificação Internacional de Doenças (CID 10) a caracterização desse fenômeno como uma condição também conhecida como transtorno pedofílico. Trata-se de uma disfunção sexual que altera o padrão de normalidade de um indivíduo, resultando em um interesse e desejo de se envolver em atividade sexual com menores de idade. Formas de violência incluem: a) violência física, caracterizada pela ação que prejudica a integridade ou saúde corporal da criança ou do adolescente, causando-lhes sofrimento físico; b) violência sexual, que compreende qualquer conduta que constranja a criança ou o adolescente a praticar ou presenciar atos libidinosos, abrangendo o abuso sexual, envolvendo a utilização da criança ou do adolescente para fins sexuais, seja de modo presencial ou eletrônico, e a exploração sexual comercial, caracterizada pelo uso em atividades sexuais em troca de remuneração ou qualquer forma de compensação, independentemente ou com

patrocínio, apoio ou incentivo de terceiros, seja de modo presencial ou eletrônico. Na legislação brasileira, essa prática é considerada crime, conforme estabelecido no artigo 240 do Estatuto da Criança e do Adolescente.

No que diz respeito aos estudos científicos, as pesquisas em psicologia e psiquiatria sugerem que a pedofilia pode resultar de uma combinação complexa de fatores, incluindo predisposições genéticas, experiências de vida, influências e disfunções psicológicas. No entanto, é importante destacar que ter atração por crianças não é uma justificação para o abuso sexual infantil, que é ilegal e prejudicial. Assim, o repulsivo ato de pedofilia não se limita a ser apenas um delito, mas também é identificado como uma condição psicológica que impulsiona o agressor a cometer tais atrocidades.

Por causa da extrema seriedade desse problema, há um considerável debate em torno do perfil do perpetrador envolvido. Dessa maneira, ações investigativas voltadas para a abordagem desse comportamento são de crucial importância. No que tange aos resultados de pesquisas, estas indicam uma associação entre a pedofilia e o funcionamento cerebral. Um aspecto menos conhecido é que, dentro do campo da medicina sexual, a pedofilia é classificada como um transtorno mental. De acordo com Dunaigre et al. (1999, p. 7):

> A pedofilia consiste em manifestações e práticas de desejo sexual que alguns adultos desenvolvem em relação a crianças de ambos os sexos na prépuberdade [...] A pedofilia evoca uma história arcaica em que um impulso sexual inaceitável leva a transgressão de uma regra humanitária.

É preciso reiterar que a pedofilia deve e é considerada como um problema sério que necessita ser tratado e prevenido. Além disso, é importante buscar ajuda terapêutica para indivíduos que apresentem atração sexual por crianças, a fim de evitar que cometam crimes contra menores.

Quando se fala de abuso sexual, tal conceito geralmente está inserido quando se trata de pedofilia. Ademais, nota-se que, geralmente, há uma confusão sobre a conceituação de abuso sexual e pedofilia e, por isso, é imprescindível dissociá-los. Por um lado, o abuso sexual caracteriza-se por uma ação, seja de qualquer pessoa que tenha relação de poder ou até mesmo confiança, a qual obriga crianças e adolescentes a praticarem atos sexuais, os quais elas não têm condições de resistir, consentir ou discernir. Por outro, o pedófilo pode cometer abuso sexual por meio de um olhar, conversas com propostas maliciosas ou por qualquer mídia social.

No que se refere ao último caso, essa conduta de forçar ou coagir a criança para satisfazer seus desejos recebe penalidades, conforme pode ser encontrado em vários artigos do Código Penal, os quais serão citados:

> Artigo 218: Induzir alguém menor de 14 (quatorze) anos a satisfazer a lascívia de outrem:
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos.
>
> Artigo 218-A: Praticar, na presença de alguém menos de 14 (quatorze) anos, ou induzi-lo a presenciar, conjunção carnal ou outro ato libidinoso, a fim de satisfazer lascívia própria ou de outrem:
>
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos.

Por conseguinte, a proteção das crianças contra o abuso sexual é uma prioridade. Então, as leis foram estabelecidas em muitos países para proteger os direitos e o bem-estar dos menores, para punir aqueles que abusam deles, para garantir o tratamento adequado e a supervisão de indivíduos que apresentam risco de cometer abuso sexual infantil. Além disso, é importante notar que a perspectiva sobre a pedofilia evoluiu ao longo da história e contínua em evolução.

Os pedófilos, ao criar perfis fictícios em redes sociais e empregar uma linguagem de fácil compreensão, procuram conquistar a confiança de crianças e adolescentes. O estudo visa ilustrar a proteção integral garantida pelo ECA, com o objetivo de salvaguardar a criança e o adolescente contra atos prejudiciais à sua integridade, independentemente do meio em que ocorram, desde que possuam a característica de causar dano à criança ou adolescente (CABETTE, 2015).

No que se refere ao padrão comportamental, as ações dos pedófilos podem ser caracterizadas como manipuladoras e sedutoras. Assim, a dinâmica de poder do agressor sobre a vítima revela-se na dominação psicológica e física da criança. Essa relação assimétrica é construída sobre segredos, manipulação e coerção por parte do abusador.

Dessa maneira, a confiança depositada pela criança facilita que o pedófilo exerça sua influência (conforme MACHADO, 2013). Quando uma pessoa nutre fantasias ou desejos sexuais direcionados a crianças com menos de 11 anos ou adolescentes que, frequentemente, carecem de informações adequadas sobre sexualidade, ela pode ser clinicamente classificada como pedófila.

Assim, os crimes oriundos da pedofilia, como, por exemplo, o abuso sexual de crianças é estritamente ilegal. Além disso, conforme mencionado, as leis definem que pessoas cuja idade

é anterior aos 11 anos não têm discernimento para a concessão de atividades sexuais. Portanto, qualquer envolvimento sexual com uma criança abaixo da idade mencionada é considerado crime. Nessa perspectiva, no que tange à proteção das Crianças da exploração sexual, é imprescindível a inclusão de medidas que possibilitem uma conscientização acerca do assunto, a fim da prevenção de abusos, como, por exemplo, uma educação pública crítica, programas de conscientização e intervenção precoce.

Já no que diz respeito às pessoas pedófilas é preciso a viabilização da prevenção, tratamento e punição. Ademais, é preciso salientar que alguns sistemas legais também oferecem tratamento terapêutico para indivíduos que têm atração sexual por crianças, com o objetivo de prevenir que cometam crimes sexuais contra menores.

Além disso, é importante lembrar que a pedofilia em si não é ilegal, uma vez que se refere à atração sexual e não à ações criminosas. No entanto, qualquer ato sexual envolvendo crianças é estritamente proibido e é punido pela lei.

Dessa forma, o cerne do direito em relação à pedofilia é tanto a proteção das crianças, quanto a punição daqueles que cometerem crimes sexuais contra elas. A lei considera o abuso sexual infantil como uma violação grave dos direitos das crianças e busca ativamente prevenir e combater esse tipo de crime.

O Código Civil, em seu artigo 1.º preceitua: “Toda pessoa é capaz de direitos e deveres na ordem civil”. Artigo 2.º “A personalidade civil da pessoa começa do nascimento com vida; mas a lei põe a salvo, desde a concepção, os direitos do nascituro”. (BRASIL, LEI Nº 10.406, 2011, p.225). Considerando tais disposições da legislação, percebe-se que é garantido que a pessoa deve receber atenção do ordenamento jurídico durante toda a sua vida. Portanto, a criança e o adolescente são detentores de direitos.

Na Legislação Brasileira, a última modificação do Código Penal em relação aos crimes (especialmente, sexuais) cometidos contra crianças e adolescentes reduziu o número de abusos infanto-juvenil. Isso aconteceu devido ao enrijecimento das legislações conforme disposto na Lei n° 12.015/2009, que alterou os artigos 240 e 241 e ainda recepcionando as alíneas do Estatuto da Criança e do adolescente.

Similarmente, o art. 227 da Constituição Federal/88 dispõe que é dever da família, do Estado e da sociedade de garantir ao menor os direitos fundamentais com absoluta prioridade, quanto à vida e à saúde, à dignidade, a educação, ao alimento e ao lazer, à cultura, ao respeito, à liberdade e a convivência familiar. (BRASIL, Vade Mecum, 2012). O Ordenamento jurídico brasileiro não possui regulamento próprio para tais atos no Código Penal, sendo designada a prática da pedofilia consta presente em outro artigo do Código Penal, possuindo outra designação, o de crimes sexuais praticados contra vulneráveis. O crime sexual que é praticado contra vulneráveis se encontra no Código Penal por meio do artigo 217-A, do CP, no qual constitui-se pela obtenção de conjunção carnal ou práticas de atos libidinosos com menor de catorze anos, vulneráveis, contendo como pena a reclusão de oito a quinze anos.

Além do artigo 217-A, do CP, o artigo 218 ao 2018-C trata sobre a corrupção de menores (Art. 218, do CP), satisfação de lascívia na presença de vulneráveis, crianças e adolescentes (Art. 218-A, do CP), favorecimento da prostituição ou alguma outra forma que expõe sexualmente de criança ou adolescente ou de vulnerável (Art. 218-B, do CP) e divulgação de cenas de estupro ou de cenas de estupro de vulnerável, de cena de sexo ou pornografia (Art. 218-C, do CP).

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: (Incluído pela Lei nº 13.718, de 2018)Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (Incluído pela Lei nº 13.718, de 2018) Aumento de pena (Incluído pela Lei nº 13.718, de 2018) § 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação. (Incluído pela Lei nº 13.718, de 2018) Exclusão de ilicitude (Incluído pela Lei nº 13.718, de 2018) § 2º Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos. (Incluído pela Lei nº 13.718, de 2018).

Atualmente, devido ao Projeto de Lei nº 4.299/20 proposto pela Deputada Rejane Dias (PT-PI), foi proposto a tipificação do crime de pedofilia no Código Penal. Isso ocorreu na tentativa de conter essa prática considerada como doença, fazendo com que os autores desse ato criminoso sejam punidos de maneira eficaz.

De acordo com Castiglione (2016, online): “De fato, analisando-se a realidade brasileira é possível concluir que apenas uma legislação mais rígida não soluciona o problema

da pedofilia e da exploração sexual infanto-juvenil. Avanços nas políticas públicas de enfrentamento são indispensáveis".

Deste modo, o autor enfatiza a importância da união dos poderes para criar iniciativas efetivas no combate às diversas formas de violência contra crianças. Ademais, ele destaca a necessidade de reforçar as garantias dos direitos presentes no Estatuto da Criança e do Adolescente, reconhecendo que a simples existência legal desses direitos não assegura, por si só, a proteção adequada contra abusos sexuais a menores.

2.1 PEDOFILIA NO ÂMBITO VIRTUAL

Na época atual, o uso da tecnologia, principalmente a *internet*, se caracteriza como uma forma de subsistência da sociedade. Apesar da tecnologia ter facilitado o cotidiano de várias pessoas, também acabou trazendo diversas problemáticas, muitos deles de difícil solução.

Crimes virtuais são ações criminosas praticadas virtualmente. Assim, a Legislação Brasileira conceitua de crime virtual (conhecido também como crime cibernético) as ações criminosas em que os indivíduos utilizam computadores ou aparelhos conectados para atacar vítimas. Acerca dos crimes advindos do ambiente virtual, destaca-se a pedofilia, crime que vem disseminando em grande e rápida proporção em todo país.

As buscas e descobertas realizadas na rede são extremamente rápidas. Isto porque são vários os meios tecnológicos presentes na sociedade, por exemplo, canais de televisão aberto e a cabo, recursos de multimídias e a ferramenta mais utilizada, a *internet*. A realidade atual faz com que as pessoas estejam mais informadas e atualizadas nesse mundo de mudanças e avanços tecnológicos. Um problema contemporâneo é a criminalidade virtual, que vem ampliando na medida em que as redes tecnologias se expandem. Além disso, a *internet* está se tornando cada vez mais acessível para todos, inclusive, para crianças e adolescentes.

Verifica-se que o crime de pedofilia no âmbito virtual vem sendo cometido com muita frequência, tendo em vista que a *internet* é liberada para todos e, com isso, crianças e adolescentes que fazem uso de redes sociais ficam muito expostas. Então, os pedófilos se aproveitam da "liberdade" da *web* e das redes sociais para criar perfis falsos e se passam por

crianças ou adultos a fim de amizade ou paquera.

Conforme mencionado, a pedofilia é um desejo sexual e atração por crianças e adolescentes e se enquadra em violência sexual infantil. Além disso, ela é conceituada sobre qualquer tipo de ato ou jogo sexual entre adultos, adolescentes ou crianças, cujo objetivo principal é satisfazer os prazeres sexuais do adulto devido a estimulação sexual das crianças e adolescentes (BRASIL, 2007). Nesse viés, esse crime se disseminou até mesmo no mundo virtual.

Em consequência disso, os chamados "pedófilos" aproveitam da vulnerabilidade e inocência de crianças e adolescentes a fim de obter sua confiança, fazendo com que acreditem ser a internet um mundo "totalmente seguro". Nessa ocasião, dá-se início às chamadas práticas de pedofilia (COUTINHO, 2011; MORAIS, 2019). Neste tipo de violência, o agressor geralmente usa da força, ameaçando e induzindo a vontade da vítima.

Esse tipo de violência afeta diretamente a saúde física e mental de crianças e adolescentes e intervém em seu desenvolvimento físico, psicológico, moral e sexual. Assim, é imprescindível entender que a pedofilia e a pornografia infantil são diferentes.

Por um lado, a pedofilia é uma doença, um transtorno psíquico, sendo que o indivíduo tem desejos sexuais por crianças e adolescentes, de acordo com a Organização Mundial de Saúde (OMS). Dessa forma, um pedófilo não é considerado um criminoso, porém se exterioriza sua patologia e vem a praticar tais atos que se enquadram como dispositivos legais, previstos no ordenamento jurídico, ele passa a ser um criminoso. Para o crime se caracterizar não é necessário o ato sexual, sendo suficiente a tipificação da conduta, a comercialização, divulgação de fotos vídeos pornográficos que envolve crianças e adolescentes, conforme a legislação prevê.

Por fim, é importante ressaltar que à medida c do avanço tecnológico, os crimes cibernéticos também obtiveram espaço no ambiente virtual. Diante essa evolução, os pedófilos aproveitam do ambiente virtual para comercializar, vender fotos e vídeos de crianças e adolescentes, onde essas crianças e adolescentes têm os seus direitos violados. Isto posto, observa-se um paradigma onde a prática de pedofilia ganha novo cenário de execuções, concluindo-se, que a internet virou um ambiente para práticas de vários atos ilícitos.

3 COMBATE AOS CRIMES DE PEDOFILIA VIRTUAL: OS MEIOS LEGAIS PARA ENFRENTAMENTO

3.1 DA PROTEÇÃO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Devido ao fácil acesso e surgimento de novas tecnologias, aumentou a discussão sobre a regulamentação de dados pessoais na *internet*, a qual envolve a questão da proteção da privacidade e intimidade de crianças e adolescentes. Essa discussão é substancial, pois a a criminalidade virtual, que é considerada um problema contemporâneo, vem ampliando na medida em que as redes tecnológicas se expandem. Além disso, a *internet* está se tornando cada vez mais acessível para todos, inclusive, crianças e adolescentes.

Diante da importância que o uso da tecnologia tem no dia a dia de adultos e crianças, a sociedade tornou uma conduta habitual a prática de consentir a disponibilização de dados pessoais para garantir o acesso e a utilização de diversas plataformas virtuais. Diante disso, algumas legislações previstas, como a Lei Geral de Proteção de Dados Pessoais, buscam regular o poder dos provedores no controle dos dados e informações pessoais.

Assim, a cada interação pessoal que se tem com a *internet* produz informações e dados que permitem identificar e individualizar os internautas, possibilitando que o usuário seja ininterruptamente identificado e vigiado tanto pelos provedores, como também pelo mercado e por outros usuários, públicos ou privados.

No que tange à proteção de dados pessoais, aa Constituição Federal do Brasil em seu artigo 5º, inciso X, traz que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".Assim, o direito de imagem se torna irrenunciável, inalienável, intransmissível, porém é disponível. Apesar da sua disponibilidade, é um direito que não pode ser utilizado por terceiros sem a devida autorização/licença de seu titular. Então, o direito de Imagem é de extrema importância e, como já foi exposto, está previsto como direitos fundamentais no rol dos cidadãos. Assim, sobre a proteção à imagem, de acordo com ocódigo civil em seu artigo 20º:

> art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

Analogamente, a Lei N° 13.709, sancionada em 14 de agosto de 2018 e conhecida como Lei Geral de Proteção de Dados, tem como objetivo resguardar os direitos fundamentais de liberdade e privacidade, bem como o desenvolvimento pessoal no ambiente digital, regulamentando o tratamento de dados pessoais tanto de pessoas físicas quanto jurídicas, conforme estabelece seu Art. 1°.

Essa legislação, embasada em princípios protetivos, visa criar um ambiente digital mais seguro, estabelecendo diretrizes a serem seguidas ao lidar com informações individuais. Contudo, ela define categorias específicas para os dados pessoais, a saber: Dado pessoal, Dado pessoal sensível e Dado anonimizado, todos sujeitos à proteção legal.

Dentro desse contexto, entende-se que o dado pessoal é aquele que pode ser identificado por meio de elementos específicos, como o Cadastro de Pessoas Físicas (CPF) ou Registro Geral (RG), que são inerentes a um indivíduo, estabelecendo sua identidade como brasileiro. Também são consideradas informações identificáveis, aquelas que possibilitam a identificação do indivíduo, como endereço residencial, históricos de pagamento, número de telefone, endereço de protocolo de internet, "*cookies*" e outros.

A Lei Geral de Proteção de Dados Pessoais trouxe como inovação normas específicas para definir os alcances e condições para a aquisição, guarda e tratamento das informações pessoais. Assim, ela garante a consulta gratuita e facilitada da integralidade dos dados pessoais, não alteração, “exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (CUSTÓDIO; CONRAD, 2022).

No artigo 14, caput, da referida lei, destaca-se a orientação de que os dados de crianças e adolescentes devem ser tratados de acordo com o interesse deles. Todavia, a legislação não fornece esclarecimentos detalhados sobre como diferenciar o tratamento de informações entre crianças, adolescentes e adultos em geral. A única ressalva apresentada na lei estipula que, para o tratamento de dados de pessoas de 0 a 11 anos incompletos, é necessário obter consentimento específico de um dos pais ou representante legal, limitando a coleta, forma de obtenção e finalidade de utilização desses dados (BRASIL, 2018).

A ausência da exigência de consentimento dos pais para o tratamento de dados sensíveis de adolescentes os torna mais vulneráveis à ataques. Isso ocorre porque não há um controle efetivo por parte dos responsáveis legais sobre as atividades *online* dos adolescentes,

expondo-os a diversos tipos de violência na rede, como abuso, aliciamento, disseminação de exploração sexual/comercial *online* e *cyberbullying* (CUSTÓDIO; CONRAD, 2022).

Cada dia demanda novas adaptações sociais e, apesar de ser uma legislação recente, a Lei Geral de Proteção de Dados (LGPD) apresenta aspectos cruciais para assegurar a segurança jurídica dos usuários do ambiente virtual. Este é um espaço de acesso livre e voluntário, sem restrições de faixa etária, o que engloba desde crianças até adultos.

Diante desse cenário, é notável que crianças e adolescentes fazem parte do contingente que utiliza diariamente a *internet* e os meios digitais. Embora alguns desses meios possuam classificações indicativas, muitas vezes esses usuários mais jovens não estão sob supervisão efetiva de pais ou responsáveis, tornando-se vulneráveis à ataques, crimes virtuais e vazamento de dados pessoais.

Essa vulnerabilidade não decorre apenas da falta de consciência dos pais ou responsáveis sobre os perigos *online*, mas também da falsa sensação de segurança que a *internet* pode proporcionar. Muitos pais acreditam erroneamente que é mais seguro deixar seus filhos entretidos com dispositivos dentro de casa. No entanto, essa sensação ilusória de segurança apresenta riscos, considerando que, ao utilizar aplicativos e *softwares*, frequentemente é necessário fornecer dados pessoais, criar contas e consentir com o uso de "*cookies*".

Além disso, os usuários, independentemente da idade e de forma assídua preenchem formulários *online* sem compreender totalmente a finalidade da coleta e o destino de seus dados. Por exemplo, ao aceitar "*cookies*" durante o *login* em *sites* e aplicativos, muitos usuários fazem isso sem entender completamente a função desses elementos. Os "*cookies*" podem ser uma ameaça à segurança, pois, embora facilitem a navegação, também têm a capacidade de rastrear atividades.

Portanto, destaca-se a importância de os adultos, pais ou responsáveis supervisionarem as atividades *online* de crianças e adolescentes, uma vez que, em muitos casos, eles concedem permissões sem compreender plenamente as implicações.

Por fim, fica a indagação sobre se as lacunas evidentes na Lei Geral de Proteção de Dados, caso sejam corrigidas, podem impedir situações desse tipo. Caso contrário, podem acarretar repercussões ao longo da vida da criança. Afinal, a finalidade dos dados expostos permanece incerta. Nesse contexto, a criança se torna vítima de violência ao ter seus dados utilizados de maneira indevida.

3.2 DA INFILTRAÇÃO DE AGENTES DE POLÍCIA NA INTERNET

Restando evidente, pedofilia virtual crime que são cometidos pelo agente junto à rede mundial de computadores, e que crianças e adolescentes são vítimas. Diante da facilidade de acesso e a criação de vários perfis sem a exigência de comprovação da verdadeira identidade, houve a possibilidade de infiltração virtual de agentes policiais disfarçados, para a investigação de crimes contra a dignidade sexual de crianças e adolescentes.

Compreende-se o anonimato como uma prática intrínseca ao ambiente virtual, especialmente na *Deep Web*, então, torna-se necessário reavaliar as abordagens tradicionais de prevenção e repressão a delitos, uma vez que essas práticas foram concebidas com foco predominante em investigações no espaço físico. Além disso, é empiricamente observável que os crimes ocorridos no ambiente virtual apresentam um dinamismo singular, o que sugere que métodos convencionais de repressão podem se revelar inadequados.

Diante da complexidade e abrangência de certos delitos cibernéticos, especialmente quando se considera a instabilidade das evidências deixadas pelos autores, suscetíveis a serem facilmente apagadas, alteradas ou perdidas surge a prática da infiltração policial em ambientes virtuais. Com a justificativa de investigar crimes relacionados à dignidade sexual de crianças e adolescentes perpetrados no meio virtual, a Lei nº 13.441/17 introduz no Estatuto da Criança e do Adolescente os artigos 190-A, B, C, D e E, regulamentando a infiltração virtual de agentes policiais (BRASIL, 2017).

A Lei Nº 13.441, DE 8 DE MAIO DE 2017, altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) para prever a infiltração de agentes de polícia na *internet* com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

Assim, a infiltração é uma técnica excepcional e subsidiária de investigação criminal. Dessa maneira, após prévia autorização judicial e com uma finalidade investigativa, um agente público é infiltrado na *internet* a fim da obtenção de provas que possibilitem prevenir, detectar, reprimir e, de modo consequente, combater a atividade criminosa dos agentes infratores

virtuais. E, com a obtenção de provas suficientes, há instauração da fase processual (FEITOSA, 2009; SALES, 2017).

É preciso destacar que a nova modalidade de infiltração, a qual podemos denominar como “virtual”, deverá ser realizada por um agente policial devidamente treinado para tal desígnio. Isto é, esse profissional deve apresentar aspectos psicológicos condizentes com a complexidade da operação, perfil intelectual adequado para o correto desempenho das tarefas inerentes ao plano operacional, conhecimentos avançados em matéria cibernética e a capacidade de inovar em situações de extrema fragilidade no tocante ao sigilo do trabalho encoberto (PEREIRA, 2017, p.109).

No que concerne ao respaldo da Lei, é imprescindível mencionar que a Lei nº 13.441/17 veio para inovar o ordenamento jurídico brasileiro, proporcionando a infiltração de agentes policiais no ambiente virtual para o combate de crimes aliados à pedofilia. *In casu*, o legislador, ao analisar as dificuldades enfrentadas na obtenção de provas por métodos convencionais e diante da gravidade dos atos perpetrados contra crianças e adolescentes, reconhece a necessidade de estabelecer alternativas para a comprovação da autoria e materialidade de crimes cibernéticos que atentam contra a dignidade sexual dessa parcela vulnerável da sociedade.

Além disso, a infiltração virtual se destaca por sua alta relação de custo-benefício para o Estado. Dada a necessidade de profissionais altamente capacitados, considerando as vastas dimensões geográficas do Brasil, torna-se pouco viável realizar infiltrações em ambientes físicos fora dos grandes centros urbanos. Os criminosos, especialmente aqueles envolvidos no compartilhamento de pornografia infantil, não se limitam a essas áreas metropolitanas.

Nesse contexto, a investigação desses crimes é extremamente complexa, uma vez que os criminosos interagem em redes sociais fechadas, principalmente na *Deep Web*, usando pseudônimos e códigos. Tornando-se, assim, desafiador para a polícia descobrir onde essas comunicações e a troca de material de pedofilia estão ocorrendo. Nesse viés, a única maneira de descobrir a verdadeira identidade dos criminosos e reunir evidências é permitir que policiais ingressem e participem por um período dessas redes.

Outro fator a ser observado é que a aplicação da infiltração policial enfrenta desafios, especialmente, no que diz respeito à sua duração, pois o prazo máximo de 720 dias concedido pela lei revela-se inadequado diante da dinâmica particular dos crimes virtuais, que difere significativamente dos delitos ocorridos em ambientes físicos. Isso se deve às complexidades inerentes à investigação e infiltração em organizações criminosas, desafios que se tornam

exponencialmente mais intensos em um ambiente tão desconhecido como a *Deep Web*, cuja extensão é por si só desconhecida e a navegação é obscura.

Conclui-se, portanto, que a investigação policial é um instrumento crucial para desvendar crimes virtuais, especialmente, aqueles cometidos na *Deep Web*. Dessa forma, é imperativo investir na capacitação contínua dos agentes policiais e na atualização constante da legislação nacional para enfrentar as organizações criminosas que se valem do anonimato para perpetrar uma variedade de delitos.

3.2.1 LEI CAROLINA DIECKEMAN

É evidente que a Legislação Brasileira vem se aprimorando na proteção da imagem com o objetivo de diminuir os casos de violações desse direito. Dessa maneira, é essencial o estudo do tema colocando-se em pauta os crimes que são cometidos virtualmente e seus efeitos. No Brasil, durante vários anos, era praticamente escassa uma legislação que tipificasse condutas e protegesse as vítimas desse crime, mas só ocorreu quando uma atriz famosa teve suas fotos íntimas vazadas. Diante isso, o Congresso Nacional viu na obrigação de dar uma resposta à população e tramitou a Lei 12.737/12. Embora criada essa legislação, é uma lei ineficaz perante os delitos virtuais. Assim, acerca da ineficácia da lei Carolina Dieckeman; Atualmente, não existe legislação que aborde eficazmente a atuação de hackers na Deep Web, deixando as autoridades sem uma base legal para conduzir investigações e aplicar punições. Como Cordeiro (2015) destaca, não há regulamentação jurídica adequada para essa ferramenta, indicando a lacuna do direito em alcançar o mundo virtual. Bezerra e Silva (2020, p. 17) corroboram, afirmando que "infelizmente não há regramento jurídico existente para tal ferramenta, concluindo-se que o direito é específico e não alcança este mundo virtual, ao menos agora, quem sabe em futuro mais próximo".

A Lei 12.737 de 30 de novembro de 2012, popularmente conhecida como 'Lei Carolina Dieckmann', foi pioneira ao abordar crimes cibernéticos, especificamente, o delito de invasão de dispositivo informático no art. 154-A do CPB. Conforme os artigos 154-A e 154-B24:

> Invasão de dispositivo informático
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação
> indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar

> vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou,
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
>
> Ação penal
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos". (BRASIL, Lei nº 12.965, 2014).

Embora represente um avanço, a lei apresenta deficiências notáveis, especialmente pela ausência de previsão para lidar com formas de violência moral decorrentes de crimes cibernéticos. A mobilização da sociedade, impulsionada pelo caso da atriz Carolina Dieckmann, influenciou a rápida aprovação da lei, mas essa pressão midiática pode ter contribuído para suas lacunas. Nessa perspetiva, é crucial uma legislação mais cuidadosamente elaborada, envolvendo juristas e especialistas, para uma proteção mais abrangente contra crimes virtuais e garantir uma abordagem mais refinada dessas questões.

Observa-se que parte da limitação da eficácia da Lei 12.737/2012 reside na condição estabelecida pelo art. 154-A do Código Penal, que exige a violação de dispositivos de segurança para caracterizar o crime. Ou seja, se a vítima não possui antivírus, *firewalls* ou outros meios que garantam a segurança de seu dispositivo eletrônico, a invasão virtual não é considerada crime, pois é necessário ultrapassar algum mecanismo de segurança.

Essa legislação foi elaborada para preencher lacunas no sistema jurídico referentes aos crimes virtuais, delineando claramente direitos, garantias e responsabilidades nos meios digitais.

No entanto, embora pareça eficaz ao abordar os direitos do usuário, ela deixa a desejar. A falta de punição por parte do Estado é uma realidade. Atualmente, existem inúmeros crimes virtuais, mas em muitos casos, ainda não há uma definição específica e regulamentação clara para esses delitos. À vista disso, a ausência de uma lei específica para tipificar esses crimes contribui para a falta de punição.

3.2.2 ESTATUTO DA CRIANÇA E DO ADOLESCENTE (ECA)

No contexto do Estatuto da Criança e do Adolescente (ECA) e da Constituição Federal (CF), é estabelecido de maneira clara que a prática de filmar, dirigir, fotografar ou reproduzir cenas pornográficas ou de sexo explícito envolvendo criança ou adolescente é crime, sujeito a penalidades, conforme o artigo 240 do ECA:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente.

Por conseguinte, o artigo 241 do ECA tem como objetivo condenar aqueles que participam desse mercado ilegal:

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Do mesmo modo, o artigo 241-B do ECA aborda acerca do uso da internet para propagar conteúdos de sexo explícito ou pornográficos, e prevê a punição para quem possuir ou armazenar tais materiais envolvendo menores:

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

O artigo 241-C do ECA trata da proteção contra montagens ou edições tecnológicas que exponham a figura de criança ou adolescente de maneira inadequada:

> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:

Ademais, o aliciamento, assédio, instigação ou constrangimento de criança ou adolescente, independentemente do meio de comunicação utilizado, é objeto de discussão no artigo 241-D do ECA:

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

Além disso, a Constituição Federal reforça a proteção à criança e ao adolescente, considerando dever da família e do Estado garantir prioridade em questões de qualidade de vida, saúde, educação e uma vida digna:

> Art. 229. Os pais têm o dever de assistir, criar e educar os filhos menores, e os filhos maiores têm o dever de ajudar e amparar os pais na velhice, carência ou enfermidade.

Desse modo, a responsabilidade dos pais na assistência, criação e educação dos filhos menores é enfatizada, conforme previsto na Constituição Federal, especialmente no artigo 227 § 4º.

4 AS DIFICULDADES DE IDENTIFICAÇÃO DA AUTORIA NOS CRIMES DE PEDOFILIA VIRTUAL

Como já foi mencionado, em virtude ao aumento constante dos crimes cibernéticos, um dos principais desafios para as autoridades de repressão reside na complexidade de identificar e punir os responsáveis por esses delitos. Isso acontece porque esses criminosos atuam de maneira oculta no mundo digital, implementando sofisticados bloqueios que dificultam significativamente essa identificação. É sabido que a abertura de um inquérito policial requer indícios suficientes de autoria e materialidade.

Portanto, as investigações relacionadas aos crimes cibernéticos precisam empregar métodos que levem à identificação do autor do delito, uma tarefa que depende essencialmente de uma infraestrutura tecnológica adequada para oferecer suporte a esse processo. Entretanto: O Estado não deve estigmatizar o indivíduo nem inferir em pessoas abstratas. A identificação

precisa do autor e a delimitação correta da infração são fundamentais para sancionar o criminoso virtual, especialmente considerando o ambiente virtual onde o crime ocorreu, marcado pela ausência da presença física do infrator (MALAQUIAS, 2015, p. 119).

Conforme destacado por Maia, existe uma insuficiência na regulamentação dos crimes virtuais diante dos desafios apresentados pela sociedade digitalizada. O autor sugere que as normas existentes não são adequadas para lidar de forma eficaz com os delitos cibernéticos. Em relação aos principais obstáculos enfrentados pelas autoridades brasileiras na investigação desses crimes, destacam-se a demora na concessão de mandados judiciais, a realização de perícias e dificuldade em obter respostas de alguns provedores de acesso e conteúdo.

Ainda sobre os desafios, a precisão na identificação e o eficiente rastreamento de infratores são desafios cruciais no cenário jurídico, tornando-se cada vez mais complexos devido ao avanço tecnológico e à globalização das atividades criminosas. Essas complexidades têm implicações substanciais para a aplicação da lei e a administração da justiça.

Segundo Almeida (2018, p. 45), "a identificação precisa e o rastreamento eficiente de infratores são fundamentais para garantir a adequada aplicação da justiça". Um dos principais obstáculos na identificação de infratores surge do uso de tecnologia avançada por parte dos criminosos, que buscam ocultar suas identidades e rastros digitais. Então, a anonimização na *internet*, o emprego de criptomoedas e as técnicas de camuflagem digital complexificam a tarefa de rastrear infratores. Conforme enfatizado pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), "a proteção da privacidade e a garantia dos direitos individuais são princípios fundamentais a serem respeitados durante o processo de identificação e rastreamento de infratores".

De acordo com Silva (2020, p. 78), "a criatividade dos criminosos na utilização de ferramentas tecnológicas para evitar a detecção representa um obstáculo significativo para as autoridades".

Destaca-se que, nas distinções mencionadas anteriormente, a atenção se volta para os crimes cibernéticos relacionados à violação de dados e informações, caracterizados pela invasão de dispositivos eletrônicos. Contudo, é evidente que existem condutas que não se enquadram nesse contexto técnico, como a pornografia infantil, grupos de *WhatsApp* com intenções criminosas, entre outros.

Assim sendo, os crimes cibernéticos abrangem uma variedade maior do que inicialmente pode parecer e não se limitam apenas à invasão de dispositivos eletrônicos, mas também à utilização desses dispositivos para fins criminosos. A natureza transnacional dos delitos contemporâneos torna desafiador rastrear infratores que atuam em diferentes jurisdições.

O *cibercrime*, por exemplo, frequentemente envolve indivíduos e grupos que operam internacionalmente, exigindo cooperação entre países e organizações internacionais. Como ressaltado na Convenção de Budapeste sobre Cibercrime (2001), "a colaboração transfronteiriça é essencial para lidar com a crescente complexidade dos crimes cibernéticos".

Outro aspecto relevante é a necessidade de equilibrar a eficácia do rastreamento de infratores com a proteção dos direitos individuais e da privacidade. O acesso à informações pessoais e a interceptação de comunicações digitais devem ocorrer de acordo com as leis e regulamentações vigentes.

Ademais, outro obstáculo relevante é abordar a "*dark web*," um ambiente virtual propício para atividades criminosas, como tráfico de drogas, armas e informações roubadas, caracterizado por um alto nível de anonimato. O acesso a essa área requer ferramentas específicas e investigar nesse ambiente demanda expertise especializada. O Ministério Público Federal destaca que "o combate aos crimes na dark web demanda recursos técnicos e humanos significativos" (Ministério Público Federal, 2018).

Nesse cenário, a capacitação contínua das equipes de investigação e aplicação da lei é crucial para enfrentar os desafios na identificação e rastreamento de infratores. O treinamento constante em técnicas de investigação digital, análise forense e uso de ferramentas tecnológicas é essencial para manter a eficácia das operações, como observa Barbosa (2019, p. 88), enfatizando que "a formação adequada dos profissionais envolvidos na investigação é um fator determinante para o sucesso na identificação e rastreamento de infratores."

A cooperação internacional desempenha um papel crucial na identificação e rastreamento de infratores que atuam em jurisdições estrangeiras. Tratados e acordos de cooperação, como a Convenção de *Budapeste* sobre *Cibercrime*, são instrumentos essenciais para facilitar a troca de informações e a colaboração entre países. Conforme destacado pelo Ministério da Justiça e Segurança Pública (2020), "a cooperação internacional é fundamental para enfrentar infratores que cruzam fronteiras."

O Brasil enfrenta desafios significativos na segurança cibernética, classificando-se como o 33º país em uma lista de 219, com uma crescente quantidade de denúncias. Há uma lacuna na infraestrutura das Polícias Federal e Civil, aliada à escassez de profissionais especializados em crimes cibernéticos (LESSA; VIEIRA, 2017).

Essa realidade evidencia a necessidade urgente de políticas públicas direcionadas à segurança, incluindo a capacitação de profissionais e a colaboração entre entes federativos para desenvolver mecanismos de identificação, especialmente diante da existência de quadrilhas especializadas em crimes cibernéticos (WENDT; JORGE, 2013).

A interação entre criminosos de diferentes estados ou países, que utilizam recursos tecnológicos avançados e criptografia, dificulta a determinação do conteúdo das comunicações entre eles. No entanto, a principal dificuldade reside não apenas na falta de normas classificatórias, mas na escassez de tecnologia e mão de obra, somada à relutância de empresas de informação em cooperar plenamente com autoridades (CRUZ; RODRIGUES, 2018).

Nessa perspectiva, os desafios na identificação e rastreamento de infratores envolvem uma complexidade que abarca tecnologia, regulamentação, ética e cooperação internacional. Uma abordagem integrada é necessária, considerando direitos individuais, proteção de dados e colaboração entre jurisdições e agências. Sob tal prospectiva, é preciso manter as autoridades atualizadas com as mais recentes tecnologias e regulamentações, para que, dessa forma, haja um enfrentamento eficaz contra o crime em um ambiente digital e globalizado (Moreira, 2020).

Nesse contexto, a rapidez na identificação e rastreamento torna-se crucial para a efetividade da justiça, impedindo que infratores escapem da responsabilização. Para alcançar isso, além dos investimentos em tecnologias avançadas, compreender as motivações e perfis dos infratores é essencial. Nesse sentido, o apoio da psicologia forense e análise comportamental é indispensável, pois auxiliam na elaboração de perfis criminais, facilitando a identificação dos responsáveis. A investigação transcende o aspecto técnico ao incluir a compreensão das motivações, proporcionando pistas valiosas (Moreira, 2020).

Além desses pontos, a conscientização pública e a participação ativa da comunidade também se configuram como recursos valiosos no processo de identificação e rastreamento. Dessa maneira, o envolvimento dos cidadãos na denúncia de atividades suspeitas e compartilhamento de informações contribui de forma significativa para as investigações. Assim, campanhas de conscientização e programas comunitários desempenham papel vital na luta contra o crime e na identificação de infratores.

4.1 O ANONIMATO POR TRÁS DA INTERNET

Tudo o que se pode acessar de maneira convencional pertence à *surface web*. Ao simples ato de abrir o navegador, inserir o endereço do *site* de pesquisa preferido e acessar redes sociais, *sites* de notícias, entre outros, caracteriza-se como navegação na *surface web*. A disseminação da *internet* também atraiu indivíduos mal-intencionados, pois o anonimato na *Webt* é mais fácil de ser mantido. Dessa maneira, o aumento dos crimes cibernéticos é notável, sendo comum que criminosos cibernéticos adaptem crimes do "mundo real" para o plano virtual, abrangendo áreas como pornografia infantil, apologia e incitação aos crimes contra a vida, entre outros (ROSA, 2019).

Além dessa camada mais “superficial” da rede, também tem uma camada mais profunda. Esta camada é conceituada de *deep web,* onde o anonimato é praticamente absoluto, com criptografia de dados e respeito ao direito à privacidade. Essa área é explorada por criminosos devido aos benefícios da criptografia, realizada em várias camadas, permitindo a prática de crimes, incluindo a presença de lojas com mercadorias ilícitas em seus catálogos e mídias de abuso sexual infantil.

Para compreender melhor o funcionamento da *deep web*, é essencial explorar o conceito de criptografia. Na vida *online*, é inevitável para um internauta compartilhar documentos ou arquivos pessoais, seja digitalizando documentos para o banco ou enviando arquivos por meio de aplicativos de mensagens para pessoas confiáveis. Nessas situações, a criptografia desempenha um papel crucial.

A criptografia é uma ferramenta essencial para a utilização da *internet*, permitindo o acesso ao dinheiro, compartilhamento de dados e impedindo que terceiros interceptem essas informações para uso indevido (DUARTE; MEALHA, 2016).

Então, a analogia das chaves de códigos destaca que apenas os usuários envolvidos na conversa possuem as chaves corretas para acessar as informações (DUARTE; MEALHA, 2016). A criptografia segue quatro princípios fundamentais: confidencialidade, garantindo que apenas o destinatário possua a chave para decifrar a mensagem; integridade, possibilitando que o destinatário identifique alterações na mensagem; autenticidade, permitindo aos usuários identificarem o emissor da mensagem; e irretratabilidade, assegurando que o emissor não possa negar a autoria da mensagem.

Devido à criptografia, não é surpreendente que indivíduos mal-intencionados explorem a *deep web* para atividades ilegais, sendo uma ocorrência frequente. Enquanto na *surface web* os vírus são uma forma comum de ilegalidade, na *internet* profunda, criminosos utilizam esse ambiente para vender produtos ilegais, incluindo mídias com cenas de abuso sexual, incluindo infantil e outros crimes reprováveis (BARRETO; SANTOS, 2019).

Portanto, nos delitos previamente mencionados, os perpetradores se beneficiam do anonimato proporcionado pela *internet* para dificultar a detecção policial, mas na *deep web*, essa tarefa se torna ainda mais desafiadora. Ao atravessar múltiplas camadas de criptografia, o rastreamento torna-se praticamente impossível, criando um ambiente propício para o consumo e compartilhamento de material pornográfico infantil (JI HOON YU, 2020).

Isto posto, a *deep web* apresenta-se como um espaço propício para o acesso à pornografia infantil, uma vez que conteúdo desse tipo na *surface web* seria rapidamente removido, seja por esforços policiais ou pela pronta denúncia da sociedade com eficácia (BARRETOS; SANTOS, 2019). Os responsáveis por *sites* na *deep web*, focados em pornografia infantil, comercializam o conteúdo físico por meio de *CDs (Compact Discs)* ou *pen drives*, além de oferecerem acesso ao material *online*. Há uma participação expressiva do Brasil no mercado negro de arquivos de abuso sexual infantil, com produção diária, comercialização e compartilhamento ocorrendo em fóruns da *internet* profunda (BARRETOS; SANTOS, 2019).

O aspecto mais preocupante da *Deep Web* reside em seu anonimato, uma vez que os usuários que a exploram raramente podem ser rastreados. Diversas ferramentas são empregadas para ocultar a verdadeira identidade e localização do usuário (ALVES, 2018, p. 126).

Assim, para viabilizar tal anonimato, as redes na *Deep Web* não se comunicam entre si e não mantêm qualquer conexão com a *internet* convencional. Esse isolamento tem o propósito explícito de tornar os usuários praticamente não rastreáveis, utilizando métodos que mascaram os números de IP, isto é, as identificações únicas de cada computador, por meio de tecnologias de computação distribuída e criptografia (ABREU; NICOLAU, 2014, p. 122).

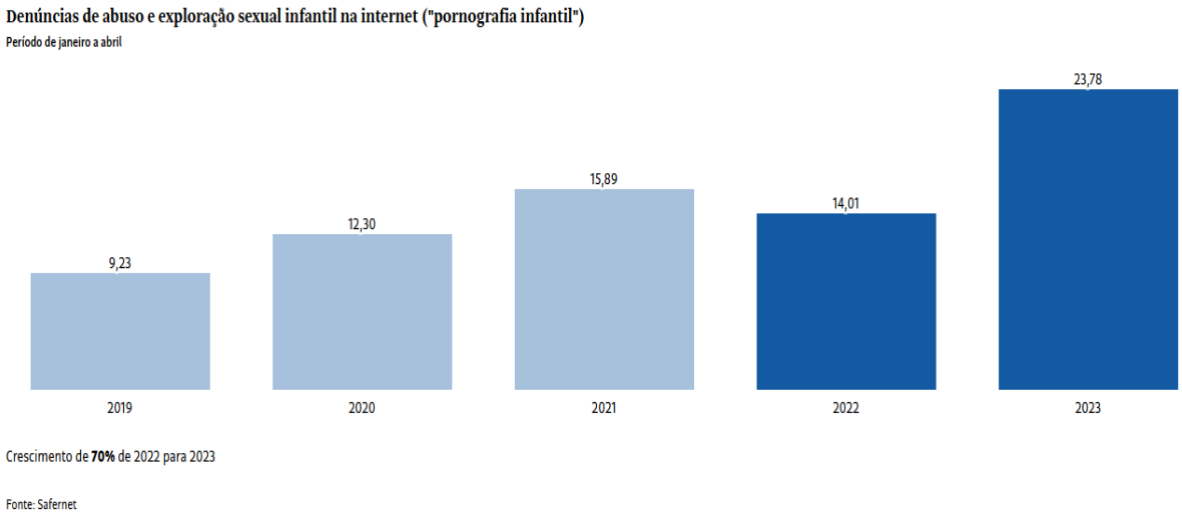
No Brasil, os casos de pedofilia virtual se multiplicaram devido aos avanços das inteligências virtuais e ao anonimato. É nítido que esses números crescem mais ao decorrer do tempo, pois os agentes criminosos se saem imunes e sem ter sua identidade descoberta. De acordo com *o* Ministério dos Direitos Humanos, levantamentos apontam que são denunciados todos os dias cerca de 366 crimes cibernéticos no Brasil e as maiores vítimas são crianças e adolescentes.

A *SaferNet* é uma rede que controla a Central Nacional de Denúncias de crimes cibernéticos. De acordo com a *SaferNet* (2023), denúncias de imagens de abuso e exploração sexual infantil reportadas por ela às autoridades cresceram 84% em um ano, entre janeiro e setembro de 2023 em relação ao mesmo período do ano passado. A *SaferNet* não utiliza mais a expressão " Pornografia Infantil ", mas sim a expressão " Imagens de Abuso e exploração Sexual Infantil" que tem o mesmo significado.

O ECA, como já citado, prevê como crime a venda ou exposição de fotos e vídeos de cenas de sexo explícito envolvendo crianças e adolescentes, a divulgação ou a posse dessas imagens. A *Safernet* recebeu total de 54.840 (cinquenta e quatro mil oitocentos e quarenta mil) novas denúncias de conteúdos com imagens de crianças abusadas sexualmente. Os dados do *SaferNet* são de acordo com os dados de operações da Polícia Federal.

Ademais, houve uma pesquisa em que aponta que as crianças, atualmente, estão acessando a *internet* por intermédio de dispositivos cada vez mais cedo e de forma excessiva. Somente esse ano, as pesquisas apontaram que 24% das crianças vêm acessando a *internet* aos seis anos de idade. No que se refere à preferência dos dispositivos eletrônicos, a maioria dessas crianças acessam a *internet* por dispositivo móvel (celular). Nesse segmento, Thiago Tavares reforça a necessidade de instrução para as crianças a respeito do uso seguro e saudável das *Web,* o aumento nas denúncias de imagens de abuso e exploração sexual infantil aponta para a necessidade de manter uma postura vigilante na proteção de crianças e adolescentes em ambientes digitais. O diálogo e orientação por parte de pais e educadores são essenciais para capacitar esse público a reconhecer situações de risco, destacando a importância da educação para o uso seguro e saudável da *internet.*

Por fim, ainda sobre a *SaferNet*, é imprescindível destacar que ela é um importante canal de denúncias, onde tornou-se a ONG brasileira de extrema referência na promoção dos direitos humanos nos ambientes digitais. Então, ela atua no combate aos crimes cibernéticos, trabalha no acolhimento de vítimas de violência *online* e em programas de educação, prevenção e de conscientização. Veja, no gráfico abaixo, os grandes índices de aumento de denúncias de pornografia infantil.



Fonte: Safernet (2023).

4.2 RESPONSÁBILIDADE DO ESTADO

Nesta seção, será abordada a responsabilidade do Estado na proteção dos direitos individuais e coletivos, assim como as abordagens adotadas para combater os crimes cibernéticos. O objetivo é explorar a capacidade jurídica do Estado, sua responsabilidade e sua atuação nesse contexto. Para fundamentar as informações apresentadas, foram realizadas pesquisas em livros, revisões bibliográficas e análises de artigos científicos, além da leitura da Constituição da República Federativa do Brasil de 1988 e do Código Penal.

A importância da capacitação jurídica específica para lidar com crimes cibernéticos é destacada, considerando a crescente influência da tecnologia em nossas vidas. A integração do conhecimento legal com a compreensão do ambiente virtual é essencial para que os profissionais possam resolver desafios relacionados aos crimes praticados na internet.

Conforme o art. 227 da Constituição Federal, é incumbência do Estado garantir à criança e ao adolescente o direito à dignidade e ao respeito, uma responsabilidade que deve se estender ao ambiente *online*. Contudo, é crucial equilibrar esse controle educacional com a preservação da privacidade e liberdade dos usuários na *internet*, garantindo o desenvolvimento autônomo de escolhas (MULTEDO, 2017).

Reconhecendo a necessidade de cautela quanto ao controle integral do Estado sobre a exposição infantil e juvenil na *internet*, medidas indiretas e legislativas são direcionadas para conscientização. Projetos de lei, como o 1746/2015 no Rio Grande do Sul e o recente projeto

de lei n° 4554/2020 do Senador Izalci Lucas, buscam proteger dados de crianças e adolescentes na *internet*, responsabilizando provedores e tornando mais graves crimes eletrônicos. Embora seja perceptível os avanços legislativos em curso, como o projeto de lei citado ainda em trâmite e campanhas governamentais, como a #NavegarNumaBoa, fornecendo dicas aos pais, a fiscalização e as legislações ainda carecem de tipificação específica para condutas abusivas *online*, regularização de propagandas para o público infantojuvenil e investimento em delegacias especializadas em cibercrimes, aspectos que demandam atenção e aprimoramento.

Apesar da extensa legislação presente em nosso ordenamento jurídico, a proteção integral de crianças e adolescentes, que deveria ser uma prioridade é, muitas vezes, negligenciada pelo controle estatal. Essa negligência ocorre mesmo diante da necessidade de resguardar os direitos fundamentais desses jovens, considerando a vulnerabilidade que enfrentam no ambiente digital e as implicações legais resultantes desse acesso.

A responsabilidade difusa, teoricamente compartilhada, não oferece uma cobertura adequada para o desenvolvimento e segurança desses indivíduos ávidos por proteção. Dessa forma, é crucial aplicar no mundo virtual alguns princípios do mundo real, respeitando legislações existentes para prevenir tratamentos desumanos, como o *cyberbullying*, que, infelizmente, se tornou comum *online*. Além disso, é vital atentar para situações aterrorizantes e constrangedoras, uma vez que o espaço *online* é vasto e pode expor os menores a riscos como a pedofilia.

Assim, é crucial a intervenção do Estado nos meios tecnológicos de produção e disseminação da informação. No entanto, essa intervenção deve ser cuidadosa, guiada pelo princípio constitucional da intervenção mínima. Mesmo reconhecendo a necessidade de intervir, é essencial manter uma abordagem pontual para inibir práticas prejudiciais resultantes do uso irresponsável da tecnologia. A maioria das condutas delituosas cometidas com o apoio da *internet* ou de computadores carece de uma tipificação específica, o que, como mencionado anteriormente, dificulta significativamente a aplicação de medidas punitivas contra tais indivíduos.

Outro aspecto a ser analisado é a escassez de delegacias especializadas em cibercrimes pelo país, totalizando apenas dezoito, concentradas nas capitais estaduais. Esse número limitado torna-se inadequado diante da extensa área territorial, o que pode resultar em dificuldades para lidar com o aumento das denúncias anuais.

A Delegacia Virtual do Ministério da Justiça[2]abrange todos os estados brasileiros, indicando uma deficiência na atuação do Estado no que diz respeito ao acesso aos serviços da justiça e à facilidade no processo de registro de ocorrências criminosas. Diante das consequências das ações desses indivíduos, torna-se imperativo alinhar as normas práticas com o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990).

Em conclusão, é evidente que o Estado desempenha um papel legítimo na defesa dos direitos dos cidadãos. Isso envolve a revisão de leis e tipificações obsoletas, bem como o reconhecimento e a penalização de novas condutas que ocorrem diariamente. O Estado não pode se manter à margem diante dos casos recorrentes existentes, sendo imperativo seu envolvimento e aprimoramento constante do arcabouço legal.

4.2.1 DESAFIOS ENFRENTADOS NO COMBATE A PEDOFILIA VIRTUAL

Para compreender os desafios associados ao combate ao comportamento criminoso relacionado à pedofilia, é essencial reconhecer que a complexidade dos crimes digitais dificulta sua eficaz abordagem. A falta de leis que garantam segurança *online* contribui para a incerteza, transformando a *internet* em um terreno desafiador para as autoridades lidarem com todos os crimes *online* (BRANT, 2003).

A legislação destinada ao ambiente virtual mostra-se impotente devido ao rápido desenvolvimento das ferramentas de tecnologia da informação. Dessa forma, a dificuldade em monitorar esse ambiente é agravada pela abundância de informações na rede, dificultando o controle rigoroso pelos servidores e provedores.

Nesse contexto, a punição por meio da legislação penal enfrenta limitações ambientais durante a investigação e processamento judicial. O anonimato dos internautas, possibilitado pela estrutura técnica da rede, complica a identificação e julgamento dos criminosos (REINALDO FILHO, 2003).

Ademais, a diversidade de locais de acesso à *internet*, como *Lan Houses* e áreas com *Wi-Fi* gratuito, dificulta a autoria devido aos números do IP. A identificação do criminoso que utiliza dispositivos móveis, como 3G, torna-se mais desafiadora devido à mobilidade desses

[2] Acessar a Delegacia Virtual do Ministério da justiça por meio do seguinte *link*: https://delegaciavirtual.sinesp.gov.br/portal/

dispositivos. Novas tecnologias também apresentam entraves ao processo de identificação (MITANI, 2012).

Assim, a dificuldade em identificar e localizar criminosos cibernéticos, aliada à necessidade de criar uma legislação abrangente e globalmente obrigatória, representa um desafio complexo (BRANT, 2003). Dessa forma, limitações geográficas e disputas entre Justiça Estadual e Federal complicam a acusação e julgamento de crimes.

No que tange à Polícia Federal, embora encarregada de investigar crimes de pornografia infantil na *internet*, enfrenta desafios significativos, incluindo a falta de ferramentas eficientes para rastreamento. A discrepância entre o vocabulário técnico de informática e a linguagem legal também representa um obstáculo, causando dificuldades na comunicação entre especialistas e delegados (MITANI, 2012).

Nessa perspectiva, o processo legislativo moroso e as discrepâncias na terminologia utilizada agravam o problema. O desafio é particularmente proeminente quando especialistas e delegados discutem relatórios técnicos durante procedimentos legais. A tradução da linguagem técnica para a linguagem jurídica, necessária para garantir a conformidade com a classificação criminal, complica a condução da investigação policial. Esse desafio se manifesta especialmente durante a elaboração de laudos periciais do material apreendido (MITANI, 2012).

Ainda sobre os desafios no enfrentamento aos crimes sexuais virtuais contra menores, um desafio significativo persiste: a obtenção das informações necessárias. Muitas vezes, os dados essenciais não são prontamente fornecidos por *sites* de hospedagem ou outros provedores de serviços. Essa lacuna na apresentação de evidências cruciais complica a localização e a confirmação da veracidade desses crimes.

Exemplificando a questão, o *Google* não colaborou prontamente ao verificar o *site Orkut* em um caso denunciado pela *ONG Safernet*. Esta situação destaca a urgência de uma maior cooperação entre empresas e organizações para prevenir crimes *online*. Dessa maneira, a falta de informações retidas pelo *Google* prejudicou a investigação conduzida pela *Safernet*, ressaltando a importância de empresas assumirem a responsabilidade pela segurança de suas plataformas e colaborarem com ONGs para proteger os usuários *online* (Lima e Mendes, 2011).

O maior desafio nesses casos é estabelecer, de forma incontestável, a verdadeira identidade do infrator. A simples instalação de um "*trojan*" no computador do usuário pode

comprometer seu sistema, muitas vezes, ocorrendo durante o *download* de aparentemente arquivos seguros, mas secretamente infectados por *software* prejudicial.

Em suma, no caso do investigado negar a autoria implica na responsabilidade dos acusadores de provar, sem dúvida, que o acusado cometeu o crime. Eles devem apresentar evidências da ausência de *software* prejudicial no dispositivo do suspeito ou demonstrar que tal *software* não poderia ter perpetrado o crime. A clareza no depoimento é crucial, pois quaisquer dúvidas podem levar à absolvição do réu, conforme previsto no artigo 386, inciso VI, do Código de Processo Penal.

4.2.2 FORMAS DE PREVENÇÃO

Inicialmente, é crucial destacar que não há uma imagem ou exemplo visual para identificar quem é pedófilo ou abusador. Devido a essa realidade, a presença ativa dos pais em todas as fases da vida de seus filhos é fundamental para evitar tais situações. É preciso compreender que o comportamento humano é complexo e, muitas vezes, apresenta nuances estranhas, pois os interesses e desejos variam consideravelmente.

O abuso sexual infantil engloba diferentes formas de contato ou exploração sexual de uma criança, seja por uma pessoa mais velha ou adolescente, abrangendo desde carícias até relações sexuais, exploração na prostituição, pornografia e outras formas de exploração sexual. Pela perspectiva da psicologia, a pedofilia é um transtorno mental no qual o indivíduo mais velho ou adolescente experimenta atração sexual exclusiva por crianças. Para prevenir tais situações, é crucial que os pais realizem um monitoramento atento de seus filhos. No entanto, é importante ressaltar que as leis destinadas a punir esses crimes precisam ser fortalecidas.

Além disso, é fundamental investir em pesquisas para desenvolver melhores formas de orientação e abordagem dessas situações. Ademais, é preciso promover palestras e diálogos abertos sobre pornografia e pedofilia e defender mudanças no sistema de justiça criminal para garantir que os condenados por abuso sexual infantil, incluindo pedófilos, sejam devidamente punidos. Como suporte, qualquer vítima de crime digital pode realizar uma denúncia em uma Delegacia Especializada em Crimes Digitais existente no Brasil.

Alternativamente, a denúncia pode ser feita em qualquer outra delegacia, caso não haja uma especializada no município da vítima. Além disso, destaca-se o projeto "Ministério Público pela Educação Digital nas Escolas", conduzido pelo Ministério Público Federal e tendo como público-alvo educadores de escolas da rede pública e privada. Estes são incentivados a realizarem atividades que ensinem crianças e adolescentes sobre o uso seguro e responsável da *Internet*. Isso contribui para evitar que se tornem vítimas ou pratiquem crimes virtuais (MINISTÉRIO PÚBLICO FEDERAL, 2018).

Dessa forma, é crucial educar os jovens sobre a importância do uso consciente da *Internet*, incentivando um comportamento responsável, reduzindo, assim, a incidência de crimes virtuais. Quando um crime virtual é encontrado ou denunciado, a delegacia responsável investigará o fato. Ao concluir o Inquérito Policial, os autos serão encaminhados ao Ministério Público para iniciar o Processo Judicial. No entanto, é importante observar que esse processo ainda enfrenta desafios, como falta de investimento e capacitação dos envolvidos, sendo um ponto a ser atentamente analisado pelo Ministério Público e pelo governo.

5 CONSIDERAÇÕES FINAIS

O estudo deste trabalho concentrou-se na problemática da pedofilia no âmbito virtual. Enfatizando que, embora esse crime já fosse prevalente, o uso de tecnologias e recursos informáticos o transformou em uma mobilidade que reduz as chances de captura do criminoso, uma vez que o anonimato por traz das redes de *internet* desempenha um papel crucial na ocultação de seus rastros.

Desse modo, focando na problemática se as ferramentas de investigação existentes tem sido eficaz para identificar os agentes criminosos dos crimes de pedofilia no âmbito virtual, foi possível responder sobre a ineficácia das legislações vigentes e dos meios de investigacões ja existentes.

Assim, no crime de pedofilia realizado no formato digital, o infrator utiliza tecnologia avançada para cometer os crimes no anonimato. Deste modo, o suspeito utiliza perfis falsos e a utilização de diversos computadores e meios de comunicação, complexando o rastreamento.

Com o aumento no acesso à internet, houve a popularização da *Deep Web*. Esta, como já mencionada no decorrer deste trabalho, é uma *Web* oculta em que permite que os criminosos cometem seus crimes em diversas localidades, sem ser rastreados. Com a dificuldade na identificação dos criminosos devido ao anonimato *online*, a rápida evolução de métodos de ocultação digital e as barreiras jurídicas e técnicas, consequentemente, há um impedimento na investigação e responsabilização.

Assim, ao considerar a necessidade de combate aos crimes virtuais, destaca-se a infiltração policial como ferramenta crucial, especialmente na *Deep Web*, onde o anonimato prevalece. A legislação brasileira evoluiu ao ampliar a possibilidade de infiltração, antes restrita ao ambiente físico. Contudo, desafios persistem, como a limitação do prazo legal de 720 dias, inadequado à dinâmica dos crimes virtuais. Apesar disso, observa-se avanço na mitigação do anonimato na *Deep Web*, impulsionado pela especialização policial e conscientização legislativa sobre a necessidade de adaptação às nuances do ambiente virtual.

Entretanto, uma legislação eficaz por si só não é suficiente. São elementos crucials para conter atividades ilícitas no ambiente virtual o aprimoramento de técnicas de investigação, o desenvolvimento contínuo dos profissionais da persecução penal, a capacitação e treinamento adequados, juntamente com a conscientização dos usuários.

O anonimato na internet representa um desafio significativo, pois a falta de identificação dos criminosos dificulta a resolução de muitos crimes, tornando a legislação frágil e menos eficaz nessas circunstâncias. É relevante ressaltar que, conforme o ECA, as crianças têm total amparo de seus direitos. Nesse contexto, é incumbência do Estado, das forças policiais e do sistema jurídico manterem-se atualizados diante dos avanços tecnológicos, prevenindo o uso de métodos ainda não legislados que possam impactar a vida desses jovens.

Diante da problemática abordada sobre a capacidade do Estado em identificar agentes criminosos de pedofilia virtual, é evidente que o panorama é desafiador. Embora o avanço tecnológico proporcione ferramentas, a complexidade do ambiente digital e o anonimato dificultam a eficácia total. O Estado enfrenta o desafio de aprimorar seus aparatos tecnológicos, fortalecer a cooperação entre entidades e promover legislações que acompanhem a rápida evolução do cibercrime, visando assim a proteção efetiva das vítimas e a responsabilização dos criminosos.

É essencial destacar que a legislação contra crimes cibernéticos deve ser continuamente atualizada para enfrentar os novos desafios da evolução tecnológica. A colaboração entre legisladores, especialistas em tecnologia e direitos infantis é fundamental

para assegurar a eficácia das leis na prevenção e punição da pedofilia digital.

Além disso, a cooperação internacional desempenha um papel crucial nessa luta. Os crimes cibernéticos ultrapassam fronteiras, exigindo que os países trabalhem em conjunto para investigar e processar os perpetradores. A criação de acordos e tratados internacionais é essencial para evitar que criminosos escapem da justiça ao mudarem de jurisdição.

Isto posto, este trabalho poderá ser utilizado em futuras pesquisas para avaliar a eficácia no combate e na identificação de crimes de pedofilia no âmbito virtual, destacando a importância de legislações e técnicas de investigação utilizadas. É um tema de extrema importância e atual, a extensão desse trabalho é de extrema ênfase.

REFERÊNCIAS

ABREU, Giovanna; NICOLAU, Marcos. **A estética do anonimato na Deep Web: a metáfora das máscaras e do homem invisível aplicada ao "submundo" da internet.** Culturas Midiáticas, [S. l.], v.7, n. 1, 2014. Disponível em: https://periodicos.ufpb.br/ojs/index.php/cm/article/view/19746. Acesso em: 14/12/2023.

ALMEIDA, A. **A pedofilia online e os desafios legais no Brasil**. Editora Jurídica, 2018. p. 45-56.

ALVES, Flaviano de Souza. **A criminalidade na Deep Web.** Revista da Escola Superior de Guerra, v. 33, n.67, p. 123-141, jan/abr., 2018. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/910. Acesso em: 14/12/2023.

BARRETO, ALESSANDRO; SANTOS, HERICSON. **Deep Web: Investigação no submundo da internet.** 1. ed. Rio de Janeiro: Brasport, 2019. 170 p. v. 1. Ebook.

BARBOSA, A. L. **A formação de investigadores para o combate ao cibercrime**. Editora Jurídica, 2019.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012.**Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 02/01/2024.

_____. **Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19/12/2023.

_____. **Marco Civil da Internet. LEI Nº 12.965, DE 23 DE ABRIL DE 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 22/10/2023.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da República Federativa do Brasil, Brasília, DF, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 ago. 2023.

CABETTE, Eduardo Luiz Santos, **A pedofilia na era digital à luz do Estatuto da Criança e do Adolescente**, por Caio Tácito Griecco de Andrade Siqueira. JusBrasil.2015. Acesso em: 05/12/2023.

CABETTE, Eduardo Luiz Santos. **O novo crime de invasão de dispositivo informático.** Revista Consultor Jurídico, 4 de fevereiro de 2013.
Acesso em 15/09/2023.

CAPEZ, Fernando. **Curso de Direito Pena**l. 6ª Ed. São Paulo: Saraiva, 2003, p. 105.

CUSTÓDIO, André; CONRAD, Camila. **A Lei Geral de Proteção de Dados e o controle de dados sensíveis de crianças e adolescentes.** Revista Cognitio Juris. Ano XII, n. 43, 2022. Disponível em: https://cognitiojuris.com.br/a-lei-geral-de-protecao-de-dados-e-o-controle-de-dados-sensiveis-de-criancas-e-adolescentes/. Acesso em: 25/07/2023.

DUARTE, David; MEALHA, Tiago. **Introdução à Deep Web.** IET Working Papers Series. 2016.
Disponível em: https://run.unl.pt/handle/10362/18052. Acesso em: 14/12/2023.

HAMADA, Fernando Massami; SANCHEZ, Cláudio José Palma. **Abuso Sexual Infantil: Normatização, Internet e Pedofilia, Encontro de Iniciação Científica,** v. 3, n. 3, p. 1-18, 2007. Disponível em:
http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/1479/1412.
Acesso em: 16/09/2023.

JI HOON YU, Fernando. **Deep Web: Análise acerca do crime envolvendo pedofilia na internet.** São Paulo, 2020. Disponível em: https://jus.com.br/artigos/81817/deep-web-analise-acerca-do-crime-envolvendo- pedofilia-na-internet. Acesso em: 06/01/2024.

LESSA, Isabella Maria Beldissera. VIEIRA, Tiago Vidal. **Crimes virtuais: análise do processo investigatório e desafios enfrentados.** Disponível em:
<https://www.fag.edu.br/upload/contemporaneidade/anais/594c13e45d209.pdf>
Acesso em: 26/06/2023.

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro**. 2017, 114p. Monografia (Bacharel em Direito) – Universidade Federal do Ceará, Fortaleza-CE, 2017.

MINISTÉRIO PÚBLICO FEDERAL. **Crimes Cibernéticos – Manual Prático de Investigação.** Disponível em:
<https://www.cnmp.mp.br/portal/images/Palestras/Atua%C3%A7%C3%A3o_do_MP_no_co

mbate_aos_crimes_cibern%C3%A9ticosINFANCIA_E_JUVENTUDE.pdf>
Acesso em: 22/12/2023.

MOREIRA, P. S. **Uso de inteligência artificial na identificação de infratores: Tendências e desafios.** Revista de Tecnologia da Informação, v. 20, n. 2, p. 123-140, 2020.

MULTEDO, Renata Vilela. **Liberdade e família: limites para a intervenção do Estado nas relações conjugais e parentais.** Rio de Janeiro: Processo, 2017.

PEREIRA, Flávio Cardoso. **Agente infiltrado virtual: primeiras impressões da Lei 13.441/2017. 2017.** Disponível em: < http://www.mp.go.gov.br/revista/pdfs_12/8-ArtigoFlavio_Layout%201.pdf>. Acesso em:28/12/2023.

ROSA, NATALIE. In: **Brasil registra aumento de 1.600% em denúncias de crimes online contra mulheres.** [S. l.], 5 fev. 2019. Disponível em: https://canaltech.com.br/seguranca/brasil-registra-aumento-de-1600-em-denuncias-de- crimes-online-contra-mulheres-132103/. Acesso em: 28/12/2023.

SALES, Marciel Antônio de. **Aspectos procedimentais da infiltração no ECA. Campina Grande, 2017.** Disponível em: <https://www.editorarealize.com.br/revistas/conidif/trabalhos/TRABALHO_EV082_MD1_SA4_ID281_17082017194131.pdf>.
Acesso em: 25/12/2023.